



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/544,119	08/03/2006	Harri Vatanen	07510.0214USWO	8647
23552	7590	09/15/2008		
MERCHANT & GOULD PC			EXAMINER	
P.O. BOX 2903			SQUIRES, BRETT S	
MINNEAPOLIS, MN 55402-0903			ART UNIT	PAPER NUMBER
			2131	
			MAIL DATE	DELIVERY MODE
			09/15/2008	PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	<b>Application No.</b> 10/544,119	<b>Applicant(s)</b> VATANEN ET AL.
	<b>Examiner</b> BRETT SQUIRES	<b>Art Unit</b> 2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If no period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED. (35 U.S.C. § 133).

Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

1) Responsive to communication(s) filed on 01 August 2005.

2a) This action is FINAL.      2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

4) Claim(s) 1-31 is/are pending in the application.

4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.

5) Claim(s) \_\_\_\_\_ is/are allowed.

6) Claim(s) 1-3,5-8 and 10-31 is/are rejected.

7) Claim(s) 4 and 9 is/are objected to.

8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on 01 August 2005 is/are: a) accepted or b) objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a) All    b) Some \* c) None of:

1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

1) Notice of References Cited (PTO-892)

2) Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) Information Disclosure Statement(s) (PTO/SB/06)  
Paper No(s)/Mail Date 11/03/05.

4) Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.

5) Notice of Informal Patent Application

6) Other: \_\_\_\_\_.

***Specification***

1. The disclosure is objected to because of the following informalities: the disclosure contains a spelling error on page 8 line 8. The disclosure recites "any other tamper-proof device," this is understood to be "any other tamper-proof device." Appropriate correction is required.

***Claim Objections***

2. Claims 7, 10, and 12-13 are objected to for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claims 7, 10, and 12-13 recite "and/or," this claim language causes ambiguity in determining what elements are required by the claims. The examiner respectfully points out that for examination purposes "and/or" is construed to mean or. Appropriate correction is required.

Claim 12 is objected to because of the following informalities: claim 12 recites "a certificate related to the user of the first and/or second terminal," on page 5 line 12, claim 12 depends from claim 8 which recites "a certificate related to the user of the first terminal," on page 4 line 12 it is unclear whether the recited claim limitations are intended to refer to different certificates. Appropriate correction is required.

Claim 14 is objected to because of the following informalities: claim 14 contains the following spelling error on page 5 line 31 "the fist terminal" this is understood to be "the first terminal." Appropriate correction is required.

Claim 16 and 31 are objected to because of the following informalities: claim 16 recites "a service provider (SP) associated with the communications network (NET)," on line 14 and "a service provider (SP) associated with the communications network (NET)," on lines 15 it is unclear whether the recited claim limitations are intended to refer to different service providers. Appropriate correction is required.

Claim 31 recites "a service provider (SP) associated with the communications network (NET)," on line 11 and "a service provider (SP) associated with the communications network (NET)," on line 12, it is unclear whether the recited claim limitations are intended to refer to different service providers. Appropriate correction is required.

***Claim Rejections - 35 USC § 112***

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 13 and 30 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 13 recites the limitation "the security gateway validation information" in page 5 line 19 of preliminary amendment filed on August 1, 2005. There is insufficient antecedent basis for this limitation in the claim. Appropriate correction is required.

Claim 30 recites the improper Markush Group of "wherein the communication network is an UMTS, a CDMA, a WCDMS, an EDGE, a Bluetooth, or a WLAN network." The use of "wherein" when claiming a Markush Group is improper because "wherein"

allows for inclusion of additional unrecited elements, and therefore renders the Markush Group indefinite. Appropriate correction is required.

Claims 14 and 15 are rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential steps, such omission amounting to a gap between the steps. See MPEP § 2172.01. Claim 14 recites "wherein if the first logical channel fails during the validation procedure, the method further comprises." Claim 14 depends directly from independent claim 1 and no validation procedure steps are recited by independent claim 1. The omitted validation procedure steps are necessary for the performance of the steps recited by claim 14. Claim 15 depends directly from claim 14 and therefore also requires the omitted validation procedure steps. Appropriate correction is required.

***35 USC § 112, sixth paragraph***

4. Claims 16 and 20-27 satisfy the three-pronged analysis necessary to invoke 35 U.S.C. § 112, sixth paragraph and accordingly these claims are interpreted as means-plus-function claims. The three-pronged analysis necessary to invoke 35 U.S.C. § 112, sixth paragraph is recited below:

A claim limitation will be presumed to invoke 35 U.S.C. 112, sixth paragraph, if it meets the following 3-prong analysis:

- (A)the claim limitations must use the phrase "means for" or "step for;"
- (B)the "means for" or "step for" must be modified by functional language; and

(C)the phrase "means for" or "step for" must not be modified by sufficient structure, material, or acts for achieving the specified function.

***Claim Rejections - 35 USC § 102***

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claims 1, 6, 16, and 31 are rejected under 35 U.S.C. 102(b) as being anticipated by Hampton et al (US 5,465,290).

Regarding Claim 1:

Hampton discloses a method of confirming the identity of a telephone caller that sets up a first logical channel ("Telephonic connection between a caller and the remote station" See fig. 1 ref. no. 14 and col. 7 lines 39-40) via a communication network ("Telephone Network" See fig. 1 ref. no. 16) between a first terminal ("Telephone" See fig. 1) and a service provider ("Remote station" See fig. 1 ref. no. 14 and col. 4 lines 35-36), and identifies the identity of the user of the first terminal after the first logical channel set up via a second logical channel ("The member processor transmits caller identification information over telephonic connection between the member processor and the central station," See fig. 1 ref. nos. 12, 24 and col. 8 lines 31-36) other than the established first logical channel between the service provider and the first terminal prior

to providing any services to the user of the first terminal ("The transaction is not processed until the caller is identified." See col. 8 lines 54-67 and col. 9 lines 1-15).

Regarding Claims 16 and 31:

Hampton discloses a system for confirming the identity of a telephone caller having a communication network (NET) ("Telephone Network" See fig. 1 ref. no. 16), a first terminal (DTE) associated with the communication network (NET) ("Telephone" See fig. 1), a service provider (SP) associated with the communication network (NET) ("Remote station" See fig. 1 ref. no. 14 and col. 4 lines 35-36), a certificate service provider (CA) ("Central Station" See fig. 1 ref. no. 12 and col. 8 lines 47-54), a sender for sending a user identification request to the first terminal (DTE) or a second terminal (DTE2) ("Speaker Verification Unit" fig. 1 ref. no. 22, col. 7 lines 62-67, and col. 8 lines 1-11), and an identifier (Speaker Verification Unit" fig. 1 ref. no. 22 and col. 8 lines 46-53) for identifying the identity of the user of the first terminal (DTE) after a first logical channel has been set up via a second logical channel ("The member processor transmits caller identification information over telephonic connection between the member processor and the central station," See fig. 1 ref. nos. 12, 24 and col. 8 lines 31-36) other than the established first logical channel between the service provider and the first terminal (DTE) prior to providing any services to the user of the first terminal (DTE) based on the information provided by the certificate service provider (CA) ("The transaction is not processed until the caller is identified." See col. 8 lines 54-67 and col. 9 lines 1-15).

Regarding Claim 6:

Hampton discloses the first and second logical channels are circuit switched connections ("Telephone Lines" See fig. 1 ref. no. 16 and col. 4 lines 31-41).

7. Claims 1-2, 5-8, 10-12, 16-25 and 31 are rejected under 35 U.S.C. 102(a) as being anticipated by Ruuth (WO 02/43346 A1).

Regarding Claim 1:

Ruuth discloses a method for performing transaction security that sets up a first logical channel ("The user's terminal physically connects to the dedicated gateway server." See page 8 lines 3-7) via a communications network ("Public Land Mobile Network" and "Public Switched Telephone Network" See fig. 1 ref. nos. 7 and 9) between a first terminal ("User's Terminal" See fig. 1 ref. no. 1) and a service provider ("Bank" See page 5 lines 1-8), and identifies the identity of the user of the first terminal ("The certificates identify the user as the subject of the certificates." See page 7 lines 15-30) after the first logical channel set up via a second logical channel ("Delivery of the certificates may take place over the air using SMS route." See page 11 lines 18-20) other than the established first logical channel between the service provider and the first terminal prior to providing any services to the user of the first terminal ("The user is not able to perform a bank transaction before the user is authenticated successfully." See page 6 lines 21-24 and page 11 lines 12-31).

Regarding Claim 2:

Ruuth discloses sending a user identification request from the service provider ("The transport layer block requests the authentication of the user." See page 8 lines 9-

19) to the first terminal via the second logical channel while the first logical channel exists between the first terminal and the service provider ("The user is not able to perform a bank transaction before the user is authenticated successfully." See page 6 lines 21-24 and page 11 lines 12-31), receiving the user identification request with the first terminal while the first logical channel exists ("Information identifying the bank is delivered to the user." See page 8 lines 9-19), digitally signing the request ("The response is signed using the authentication key" See page 8 lines 9-19), sending the signed request with the first terminal via the second logical channel ("The user's terminal sends a response to the transport layer block the response having been signed using the authentication key." See page 8 lines 9-19), authenticating the user of the first terminal and verifying the digital signature ("The signature validator checks the signature in received message." See figs. 2a-2b ref. no. 31 and page 10 lines 9-23), and providing the user with services provided by the service provider via the first logical channel ("The user is now in a position to be able to access the transactional facilities made available to her by the bank." See page 11 lines 22-30).

Regarding Claim 5:

Ruuth discloses the second logical communication channel is a packet switched connection ("Delivery of the certificates may take place over the air using SMS route." See page 11 lines 18-20).

Regarding Claim 6:

Ruuth discloses the first logical communication channel is a circuit switched connection ("The user's terminal physically connects to the dedicated gateway server." See page 8 lines 3-7).

Regarding Claim 7:

Ruuth discloses arranging a security gateway forming an interface towards the first or second terminal (See fig. 1 ref. no. 13 and page 5 lines 1-8 and 16-23).

Regarding Claim 8:

Ruuth discloses identifying the service provider with the security gateway ("The transport layer block of the gateway server responds to a call initiated by the user's terminal by identifying itself with its server certificate." See page 8 lines 3-19), sending a user identification request from the service provider to the security gateway ("The gateway server may be operated by a particular organization such as a bank." See page 5 lines 1-8 "The examiner respectfully points out that the bank operating the gateway server will program the gateway server to send a user identification request, thus the user identification request was sent from the bank to the security gateway at the programming stage."), sending the user identification request from the security gateway to the first terminal via the second logical channel ("The transport layer block requests the authentication of the user." See page 8 lines 9-19), receiving the identification request with the first terminal ("Information identifying the bank is delivered to the user." See page 8 lines 9-19), digitally signing the request ("The response is signed using the authentication key" See page 8 lines 9-19), sending the signed request to the security gateway via the second logical channel ("The user's terminal sends a

response to the transport layer block the response having been signed using the authentication key." See page 8 lines 9-19), retrieving a certificate related to the user of the first terminal ("The transport layer block of the gateway server forward the authentication response to request handler which passes it to the certificate validator of the trust server." See page 8 lines 21-31 and page 9 lines 1-13), authenticating the identity of the user of the first terminal and verifying the digital signature ("The signature validator checks the signature in received message." See figs. 2a-2b ref. no. 31 and page 10 lines 9-23), and providing the user of the first terminal a service provided by the service provider via the existing first logical channel("The user is now in a position to be able to access the transactional facilities made available to her by the bank." See page 11 lines 22-30).

Regarding Claims 10-11:

Ruuth discloses the user's terminal and the gateway server use a wireless public key infrastructure (See page 6 lines 13-19).

Regarding Claim 12:

Ruuth discloses retrieving with the security gateway a certificate related to the user of the first and/or second terminal (See page 8 lines 21-31 and page 9 lines 1-13), creating and sending a validating message to the service provider ("The gateway server may be operated by a particular organization such as a bank." See page 5 lines 1-8 "The examiner respectfully points out that the bank operating the gateway server will program the gateway server to validate the user, thus the validating message was sent from the bank to the security gateway at the programming stage."), and validating the

user of the first and/or second terminal with the service provider based on the validating message and validating information (See page 10 lines 25-31 and page 11 lines 1-10).

Regarding Claims 16 and 31:

Ruuth discloses a system for performing transaction security having a communications network ("Public Land Mobile Network" and "Public Switched Telephone Network" See fig. 1 ref. nos. 7 and 9), a first terminal (DTE) associated with the communications network (NET) ("User's Terminal" See fig. 1 ref. no. 1), a service provider (SP) associated with the communication network (NET) ("Bank" See page 5 lines 1-8), a certificate service provider (CA) ("Certification Authority" See page 7 lines 15-30), sending means (SM) for sending a user identification request to the first terminal (DTE) or a second terminal (DTE2) ("Transport Layer Block" See fig. 2a ref. no. 19 and page 8 lines 9-19), identifying means (ID) ("Trust Server" See fig. 2a ref. no. 30, page 8 lines 21-31 and page 9 lines 1-13) for identifying the identity of the user of the first terminal (DTE) after a first logical channel has been set up via a second logical channel ("Delivery of the certificates may take place over the air using SMS route." See page 11 lines 18-20) other than the established first logical channel between the service provider and the first terminal (DTE) prior to providing any services to the user of the first terminal (DTE) based on the information provided by the certificate service provider (CA) ("The user is not able to perform a bank transaction before the user is authenticated successfully." See page 6 lines 21-24 and page 11 lines 12-31).

Regarding Claim 17:

Ruuth discloses a security gateway in connection with the service provider and the certificate service provider (See fig. 1 ref. no. 13, page 5 lines 1-8, page 6 lines 26-31, and page 7 lines 15-30).

Regarding Claim 18:

Ruuth discloses the security gateway is managed by the bank (See page 5 lines 1-8).

Regarding Claim 19:

Ruuth discloses the security gateway is managed by a service provider (See page 5 lines 1-8).

Regarding Claims 20-22:

Ruuth discloses the gateway server is located on the premises of the bank (See page 5 lines 16-23).

Regarding Claims 23-25:

Ruuth discloses the user's terminal and the gateway server use a wireless public key infrastructure (See page 6 lines 13-19).

***Claim Rejections - 35 USC § 103***

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

9. Claim 3 is rejected under 35 U.S.C. 103(a) as being obvious over Ruuth (WO 02/43346 A1) in view of Kremer (US 2002/0138450).

Ruuth discloses the above stated method for performing transaction security that sends a user identification request from the service provider ("The transport layer block requests the authentication of the user." See page 8 lines 9-19) to the first terminal via the second logical channel while the first logical channel exists between the first terminal and the service provider ("The user is not able to perform a bank transaction before the user is authenticated successfully." See page 6 lines 21-24 and page 11 lines 12-31), receives the user identification request with the first terminal while the first logical channel exists ("Information identifying the bank is delivered to the user." See page 8 lines 9-19), digitally signs the request ("The response is signed using the authentication key" See page 8 lines 9-19), sends the signed request with the first terminal via the second logical channel ("The user's terminal sends a response to the transport layer block the response having been signed using the authentication key." See page 8 lines 9-19), authenticates the user of the first terminal and verifying the digital signature ("The signature validator checks the signature in received message." See figs. 2a-2b ref. no. 31 and page 10 lines 9-23), and provides the user with services provided by the service provider via the first logical channel ("The user is now in a position to be able to access the transactional facilities made available to her by the bank." See page 11 lines 22-30).

Ruuth does not disclose sending a user identification request for the user of the first terminal from the service provider to a second terminal via the second channel.

Kremer discloses sending a user identification request for the user of the first terminal ("Computer Terminal" See fig. 2 ref. no. 100) from the service provider ("Financial Entity" See paragraph 115) to a second terminal ("Mobile Telephone" See fig. 2 ref. no. 170) via the second channel ("SMS via the GSM network" See paragraph 115).

It would have been obvious to one of ordinary skill in the art at the time of the invention to include in the method for performing transaction security disclosed Ruuth sending a user identification request for the user of the first terminal from the service provider to a second terminal via the second channel such as that disclosed by Kremer in order to prevent user identification information from being stolen by packet sniffing the first channel (See Kremer paragraphs 4-10).

10. Claims 26 and 27 are rejected under 35 U.S.C. 103(a) as being obvious over Ruuth (WO 02/43346 A1) in view of Lewis et al. (US 2006/0107060).

Ruuth discloses the above stated system for performing transaction security having a sending means ("Transport Layer Block" See fig. 2a ref. no. 19 and page 8 lines 9-19) arranged to send data to the first terminal ("User's Terminal" See fig. 1 ref. no. 1).

Ruuth does not disclose the sending means is arranged to send a challenge to the first terminal in the event that the logical channel set up between the first terminal and the service provider fails.

Lewis discloses a system for authenticating the user of a cellular phone having a central server (See fig. 5a) arranged to send a challenge (See fig. 5a ref. no. 507 and

paragraphs 74-75) to the user of a cellular phone during the setup of a voice channel (See paragraph 25).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system for performing transaction security disclosed by Ruuth to include sending a challenge to the first terminal when the logical channel between the first terminal and the service provider fail and the logical channel is being reestablished such as that taught by Lewis in order to prevent thieves from trapping cell phone identification data (See Lewis paragraph 25).

11. Claims 28-30 are rejected under 35 U.S.C. 103(a) as being obvious over Ruuth (WO 02/43346 A1) in view of Atkinson et al (US 2002/0012329).

Ruuth discloses the above stated system for performing transaction security that authenticates the user of a cellular phone over a wireless communications network.

Ruuth does not disclose the communications protocols being used by the cellular phone.

Atkinson discloses that cellular phones may use: TDMA, CDMA, GPRS, GSM, EDGE, UMTS, I-mode, IMT-2000, iDEN, and 3 GPP communications protocols.

It would have been obvious to one of ordinary skill in the art at the time of the invention to include in the system for authenticating a user disclosed by Ruuth operating the cellular phone using the communication protocols disclosed by Atkinson in order to allow the system for authenticating a user to be implemented on modern wireless communications networks.

***Allowable Subject Matter***

12. Claims 4 and 9 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

***Conclusion***

13. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Boesen (US 6,987,986) discloses a cellular phone having a dual line capability that allows for simultaneous voice communications over a first line and data communications over second line (See col. 2 lines 36-51). Boesen further discloses a cellular phone having a single communications line divided into channels that can be used for simultaneous voice communications and data communications (See col. 3 lines 44-51).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRETT SQUIRES whose telephone number is (571) 272-8021. The examiner can normally be reached on 9:00am - 5:30pm Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BS/

/Ayaz R. Sheikh/

Supervisory Patent Examiner, Art Unit 2131